The RIR System & Internet Governance

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Gergana Petrova | gpetrova@ripe.net | 14 June 2019

Topics Covered

- What is an RIR?

- How are IP addresses issued?

- The RIPE Database and due diligence

- Collaboration with law enforcement

- What is the multi-stakeholder model?

- Main principles for policy making

- Key arguments and dilemmas

- Why and how to get involved

The RIR System

What is an RIR?

- A Regional Internet Registry (RIR) manages the allocation and registration of Internet number resources in a particular region of the world and maintains a unique registry of all IP numbers issued.

- Number resources include:
  - IP addresses (IPv4 and IPv6)
  - Autonomous System (AS) Numbers

- Independent, not-for-profit, membership organisation

Where are the RIRs?

Core RIR Functions

- Receive large IP address blocks from IANA

  - Distribute those in smaller blocks to its members

  - Publish and maintain a list of who has which block

  - Implement the rules (policies) set by the RIPE community

- Support the infrastructure of the Internet through technical coordination

- Provide services for the benefit of the Internet community at large

IANA
(Internet Assigned Numbers Authority)
Manages global unallocated address pool

RIRs
(RIPE NCC, ARIN, APNIC, LACNIC, AFRINIC)
Manages regional unallocated address pool

allocate

assign

ISPs/LIRs

End User
(customer)

re-allocate

re-assign

ISPs/LIRs
(customer)

End User
(customer)
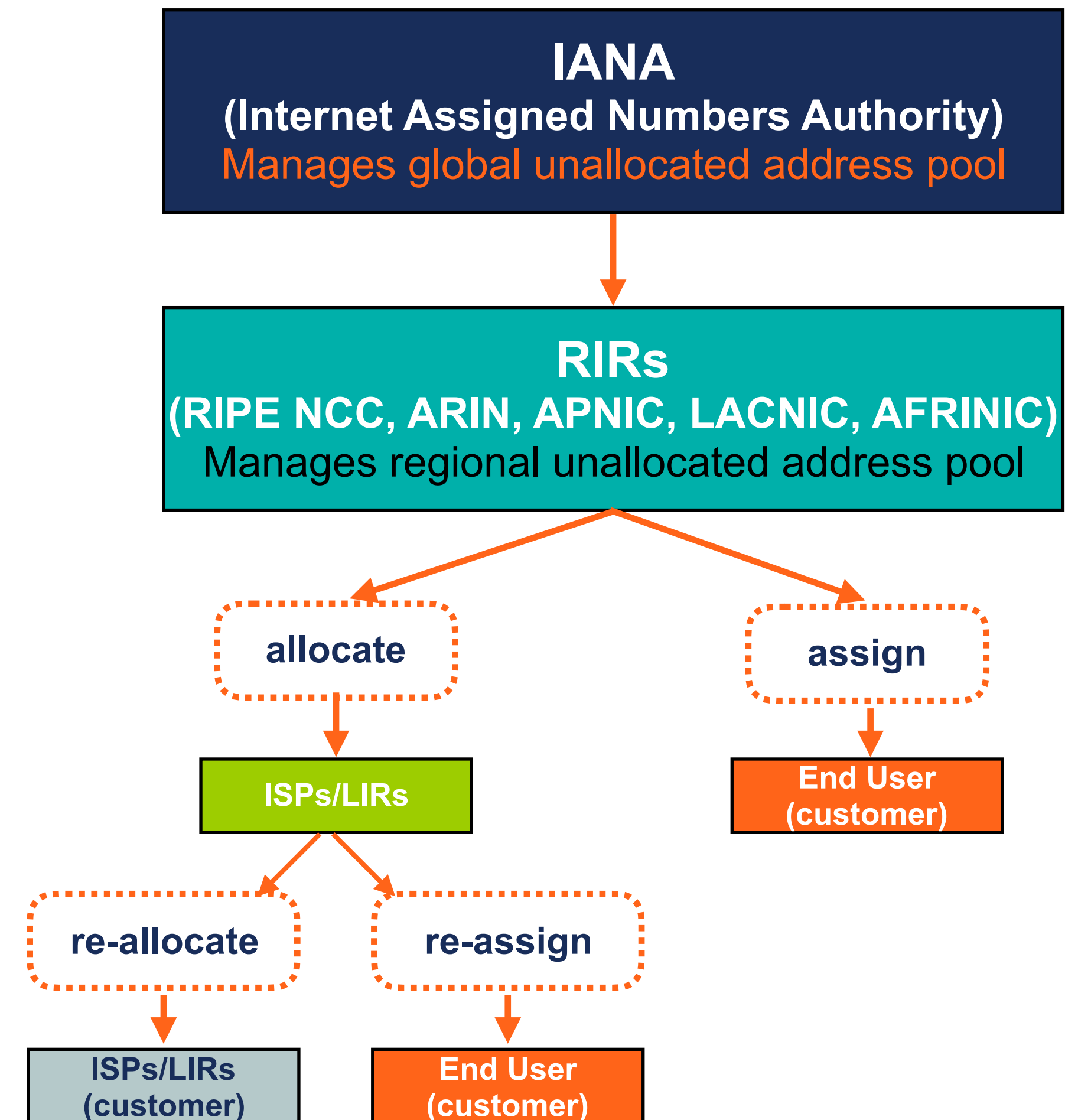
What is in the RIPE Database?

- Registration information about

  - IP addresses and AS Numbers issued by the RIPE NCC

  - IP addresses and AS Numbers issued prior to the establishment of the RIRs (legacy space)

  - Original registration date

  - Organisations that hold these resources (ORGs)

  - Points of Contact for resources or organisations (POCs)

  - Customer reassignment information (from ISPs to their customers)

  - Referential information to the authoritative RIR

www.cepol.europa.eu
194.30.123.123

```
Responsible organisation: SAREnet, S.A.
Abuse contact info: abuse@sarenet.es

inetnum:       194.30.123.0 - 194.30.123.255
netname:       NETIKER
descr:         Netiker
country:       ES
admin-c:       AJ294-RIPE
tech-c:        SM10-RIPE
remarks:       rev-srv: ns1.sarenet.es
remarks:       rev-srv: ns2.sarenet.es
status:        ASSIGNED PA
notify:        alberto@sarenet.es
mnt-by:        MAINT-AS3262
created:       2002-03-18T15:19:12Z
last-modified: 2009-09-02T15:32:15Z
source:        RIPE
remarks:       rev-srv attribute deprecated by RIPE NCC on 02/09/2009

route:         194.30.0.0/17
descr:         Clients of SARENET AS3262
origin:        AS3262
mnt-by:        MAINT-AS3262
created:       1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:32:08Z
source:        RIPE
```

What is not in the RIPE Database?

- Domain names

- Certain customer reassignments
  - Example: private residence

- Accurate geographic location of the network or end user customer

Current Challenges

- Fraudulent Activity

  - Hijacking IP address space

    ▶ Target IP address space that's not routed and not updated (mostly legacy space)

    ▶ Look for expired domain names and corporate registrations

    ▶ Make RIPE Database changes to take over the registered space

  - Attempting fraudulent transfers (huge monetary value)

  - Submitting fake documentation (passports, etc.)

  - Setting up shell companies

- Buying and selling of IPv4 address space (outside of registry system)

- Route hijacking (unauthorised use of un-routed IPv4 addresses)

- "Leasing" of IPv4 address space

How RIRs Support Law Enforcement Agencies?

- Provide publicly available Internet number resource registration data in the RIPE Database

- Provide publicly available tools to help find Internet number resource information: e.g. RIPEstat (stat.ripe.net)

- Provide tailored training courses and information sharing sessions

- Work with LEAs and the Internet community to improve the integrity and accuracy of the data

- We provide non-public data only under the request of a Dutch court order

Gergana Petrova | 14 June 2019

How Can LEAs Participate?

- Attend industry/RIR meetings

- Participate in relevant RIR Working Groups (WGs)

- Schedule training sessions with RIRs

- Submit policy proposals

  - May enhance LEA capabilities in crime-fighting for the safety and security of the Internet

    ▸ RIPE Database policies (accessibility to data)

    ▸ RIPE Database accuracy

    ▸ Verification and due diligence practices
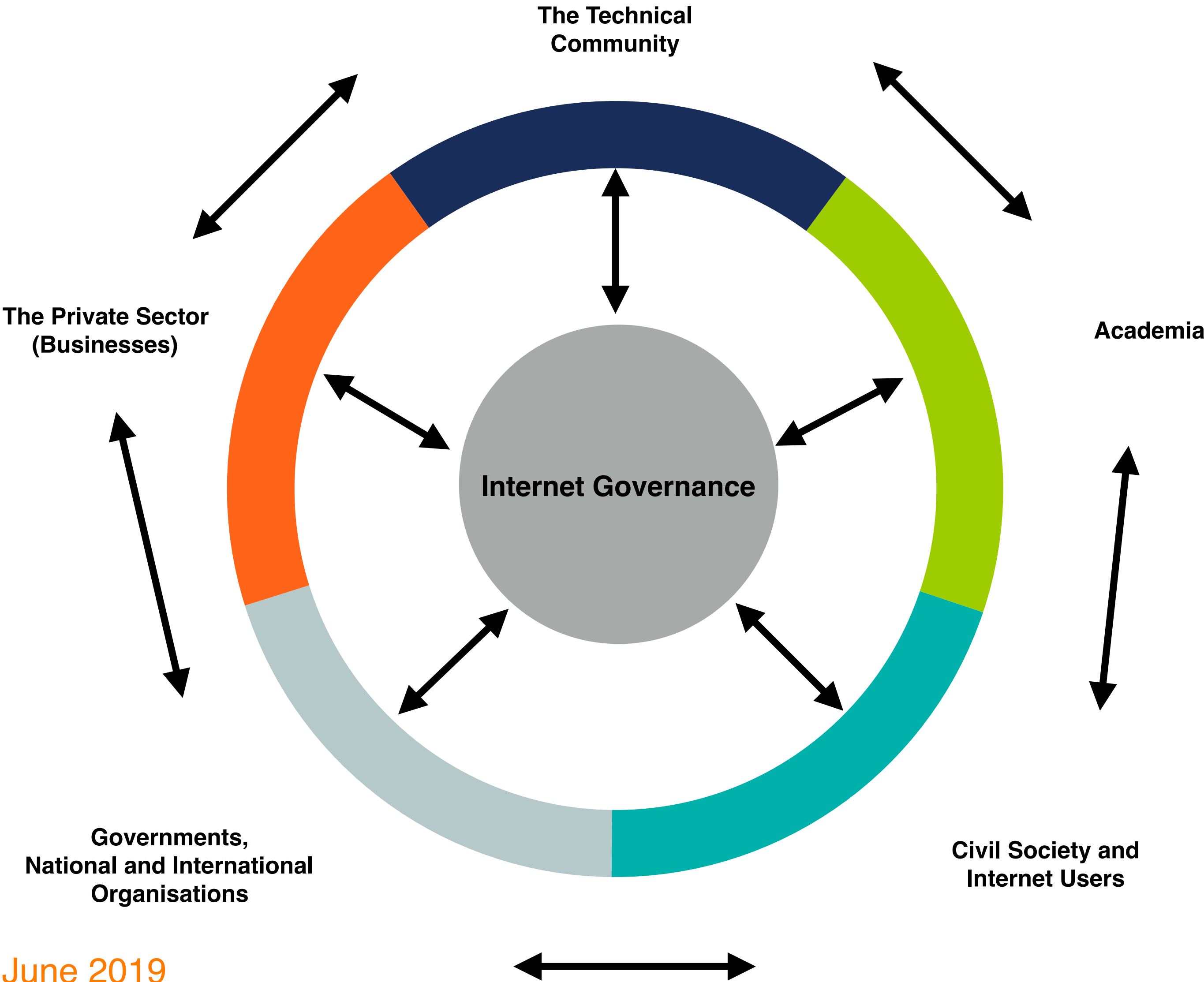
Internet Governance

What is "Internet Governance"?

"Internet Governance (IG) is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"

- World Summit on Information Society (WSIS) 2005

The Multi-Stakeholder Model

The Technical Community

Academia

The Private Sector (Businesses)

Internet Governance

Governments, National and International Organisations

Civil Society and Internet Users

Main Policy-Making Principles

- Promote the open, distributed and interconnected nature of the Internet

    - Maintain technological neutrality

- Encourage multi-stakeholder cooperation in policy development processes

- Ensure transparency, fair process, and accountability

- See NetMundial, OECD, Council of Europe, etc.

    - content.netmundial.br/internet-governance-principles/

What are the Dilemmas?

The Internet hasn't introduced anything new to governance. Our rights haven't changed.

The Internet is a fundamentally different communication system, separated from geographical reality.

Cyberspace is different than real space and requires a new form of governance.

Existing laws can be applied with minor amendments.
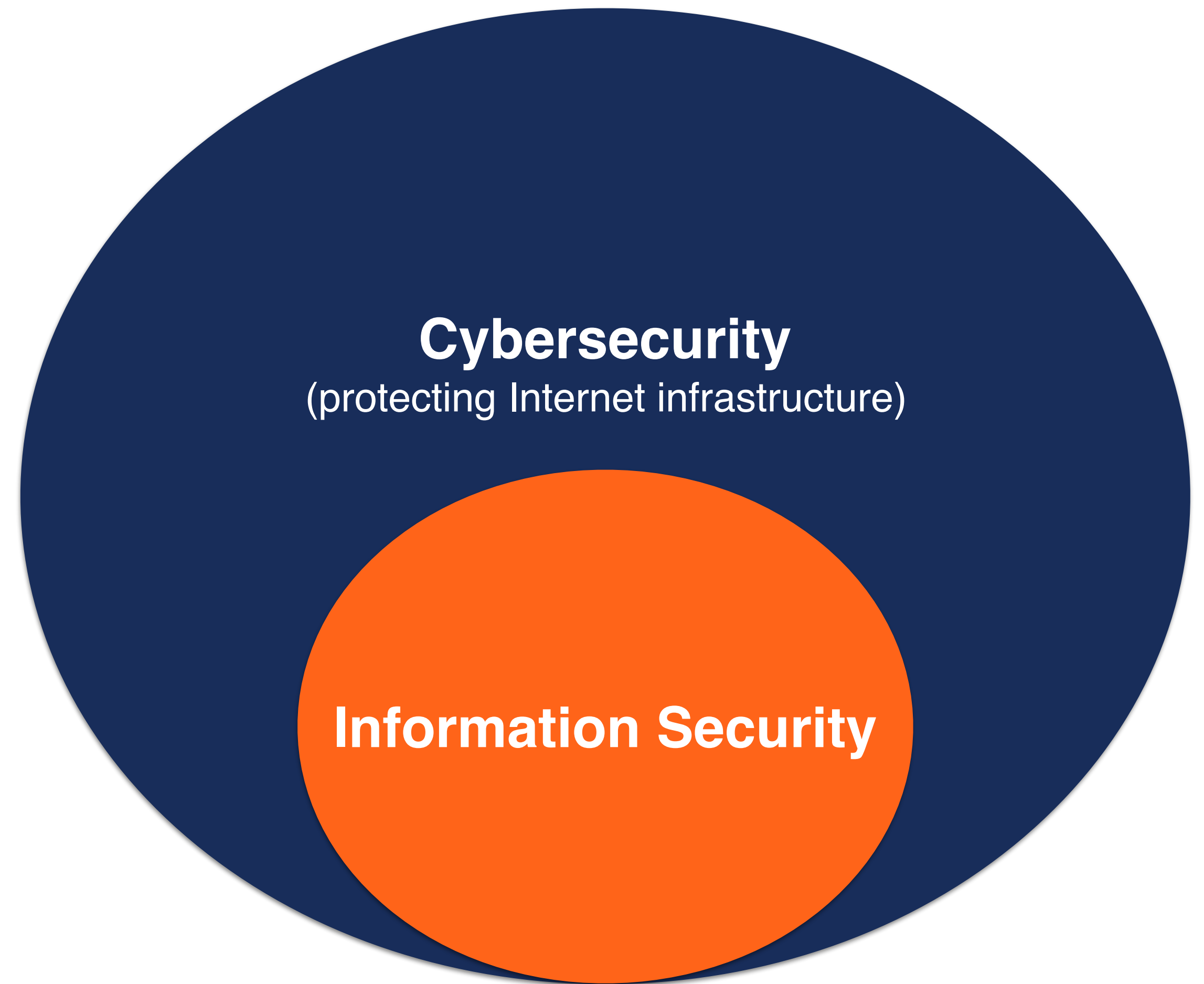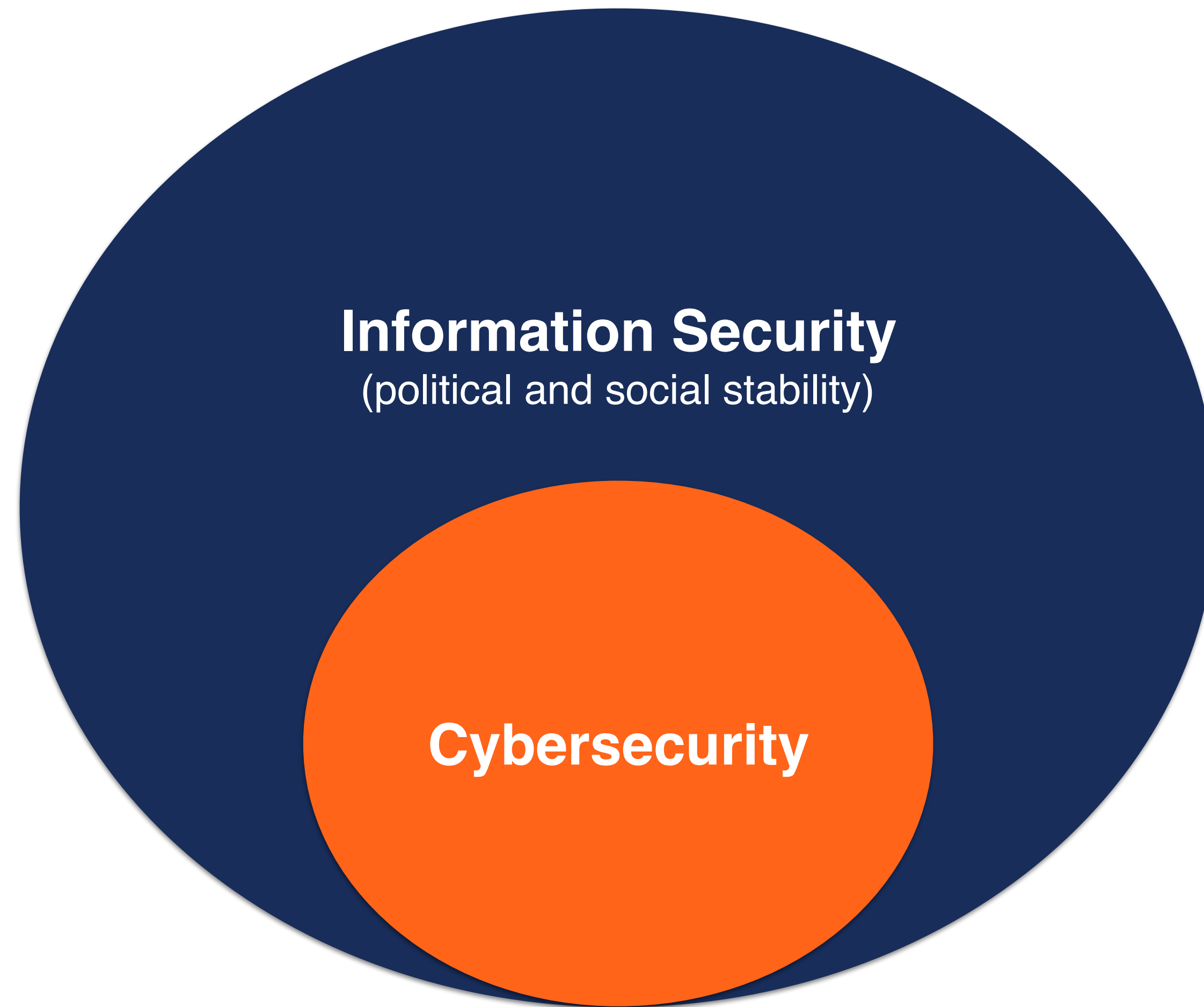
16

Centralised vs. Decentralised

Small countries have limited human and financial resources to follow IG discussions

The Internet is too complex to be placed under single governance umbrella or organisation

We want a one-stop-shop for IG issues preferably within an international organisation

We want a multi-stakeholder approach

Small But Important Differences

Information Security
(political and social stability)

Cybersecurity

Cybersecurity
(protecting Internet infrastructure)

Information Security

Content Removal

Who should be responsible for removing content / making content inaccessible on the Internet?

- Content should not be censored at all

- Access providers (ISPs, telcos)

- Content platforms (Facebook, etc)

- Law Enforcement Agencies / courts

Backdoors

Should technology companies be asked to create backdoors (write new software or modify existing software) at the request of law enforcement agencies to fight serious crime?

- Yes

- No

Cyberattacks

Who is responsible for cyberattacks (e.g. ransomware attacks such as Wannacry)?

- Government/ law enforcement

- The ICT industry (Microsoft, etc)

- CEO level at affected businesses

- IT/security departments

- Internet users

- No one is to blame: it's a part of life
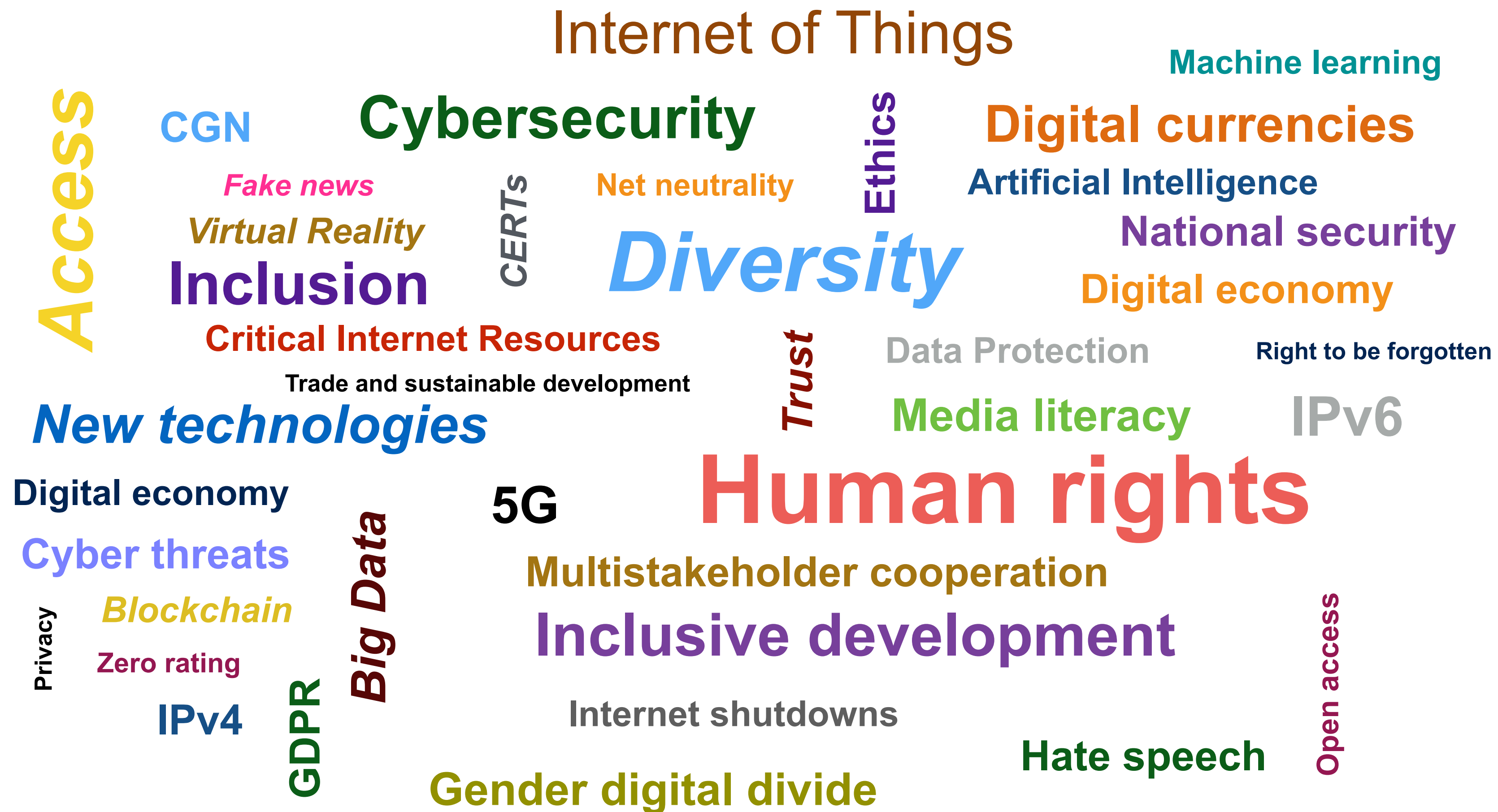
Internet Governance Forum (IGF)

- "A forum for multi-stakeholder dialogue on public policy issues related to the Internet"

- Issues like sustainability, robustness, security, stability and development of the Internet

- Open and inclusive dialogue and the exchange of ideas

- Share best practices and experiences

- Identify emerging issues and bring them to the attention of the relevant bodies and the public

- Contribute to capacity building for IG

Next IGF: 25-29 November, Berlin

intgovforum.org

Internet of Things

Machine learning

Access

CGN

Cybersecurity

Ethics

Digital currencies

Fake news

CERTs

Net neutrality

Artificial Intelligence

Virtual Reality

Diversity

National security

Inclusion

Digital economy

Critical Internet Resources

Trust

Data Protection

Right to be forgotten

Trade and sustainable development

New technologies

Media literacy

IPv6

Digital economy

Human rights

Cyber threats

5G

Big Data

Multistakeholder cooperation

Privacy

Blockchain

Inclusive development

Open access

Zero rating

GDPR

Internet shutdowns

IPv4

Hate speech

Gender digital divide

IGF Initiatives

- Regional IGFs
  - EuroDIG: 19-20 June, the Hague
  - SEEDIG: 6-8 May, Bucharest

- Multiple National IGFs
  - Albania, Armenia, Austria, Azerbaijan, Bosnia and Herzegovina, Belarus, Croatia, Denmark, Finland, Georgia, Germany, Italy, Macedonia, Malta, Moldova, Netherlands, Poland, Portugal, Russia, Slovenia, Spain, Switzerland, UK, Ukraine

- Multiple Youth IGFs

"We are having Internet Governance discussions and meetings and a very large number of people are discussing the future of the Internet who have no clue as to what the Internet is except that it is important and that they have to be involved"

- Steve Crocker

More Information

- The History of Internet Governance. By Wolfgang Kleinwächter:
  - https://www.youtube.com/watch?v=5QUrkRtC2Js

- An Introduction to Internet Governance. By Diplo Foundation:
  - https://www.diplomacy.edu/introduction-internet-governance-7th-edition

- CircleID's Internet Governance pieces:
  - http://www.circleid.com/topics/internet_governance

Questions

gpetrova@ripe.net